Exercises for Group, field and finite field

6^{th} January, 2006

1. Write the addition and multiplication tables for $GF(5) = \{0, 1, 2, 3, 4\}$

2. Find the principal remainder when $83 \cdot 54$ is divided by 7.

3. Determine whether $\left(3^{18}\right)\left(13^{35}\right) + 1$ is divisible by 17

4. Prove that $1 + x + x^3$ and $1 + x^2 + x^3$ are the only irreducible polynomials of degree 3 over $\mathbf{F}_2$.

5. Is $GF(4)$ a subfield of $GF(8)$? Explain.

6. Construct the addition and multiplication tables for the rings $\mathbf{Z}_8$.

7. Find the multiplicative inverse of 3, 6, 10 in $\mathbf{Z}_{11}$.

8. Show that the polynomials $1 + x^2$ and $2 + 2x + x^2$ over $\mathbf{F}_3$ are irreducible.

9. Factorise the polynomials $x^7 - 1$ over $\mathbf{F}_3$, $x^{20} - 1$ over $\mathbf{F}_7$ and $x^{11} - 1$ over $\mathbf{F}_5$.

10. Determine the number of primitive elements in the fields $\mathbf{F}_{10}$, $\mathbf{F}_{11}$ and $\mathbf{F}_{30}$.

11. Find the number of monic irreducible cubic polynomials over $\mathbf{F}_q$.

12. Find all the cyclotomic cosets of 2 modulo 33.

13. Let

$$f(x) = \left(2 + 2x^2\right)\left(1 + x^2 + x^3\right)^2\left(-1 + x^5\right)$$

in $\mathbf{F}_3[x]$ and

$$g(x) = \left(1 + x^2\right)\left(-2 + 2x^2\right)\left(1 + x^2 + x^3\right)$$

in $\mathbf{F}_3[x]$. Find $\gcd\left(f(x), g(x)\right)$ and $\operatorname{lcm}\left(f(x), g(x)\right)$.

14. Find two polynomials $u(x)$ and $v(x)$ in $\mathbf{F}_2[x]$ such that $\deg\left(u(x)\right) < 5$, $\deg\left(v(x)\right) < 4$ and

$$u(x)\left(1 + x + x^3\right) + v(x)\left(1 + x + x^2 + x^3 + x^4\right) = 1$$

15. Construct the addition and multiplication tables for the ring $\mathbf{F}_3[x]/\left(x^2 + 1\right)$.

16. Determine all the subfields in $\mathbf{F}_{2^{13}}$.

Reference

Raymond Hill. *A first course in coding theory.* Clarendon, 1986

San Ling and Chaoping Xing. *Coding theory, a first course.* Cambridge University Press, 2004

L R Vermani. *Elements of algebraic codng theory.* Chapman & Hall, 1996